IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	Bjorn Markus Jakobsson
Case:	39
Serial No.:	09/781,476
Filing Date:	February 12, 2001
Group:	2134
Examiner:	Ellen C. Tran

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: ______________________ Date: September 2, 2005

Title:	Encryption Method and Apparatus With Escrow Guarantees

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicant (hereinafter referred to as "Appellant") hereby appeals the final rejection of claims 1-18 of the above-referenced application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc. The assignee, Lucent Technologies Inc., is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

Claims 1-18 are pending in the application. Claims 1, 17 and 18 are the independent claims. All the pending claims stand rejected under 35 U.S.C. §102(b). The §102(b) rejection of claims 1-18 is appealed.

STATUS OF AMENDMENTS

There have been no amendments filed.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides improved encryption techniques which allow escrow guarantees on encrypted messages. For example, escrow guarantees may ensure that an appropriately-authorized government agency or other party can decrypt messages that have been encrypted by a given user, thereby giving that agency the ability to implement a "digital wiretap" of the encrypted data (Specification, p. 1, lines 9-13).

In an embodiment of the invention, a message to be transmitted through a network is encrypted such that the resulting encrypted message has associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities. Each of at least a subset of the servers of the network includes a module for checking the proof of correctness if the corresponding encrypted message passes through the corresponding server in being transmitted from a sender to a recipient through the network. The encrypted message is therefore transmitted through the network to the recipient such that in traversing the network the proof of correctness associated with the encrypted message is checked by a designated check module of at least one server of the network. If the check of the proof of correctness indicates that the proof is invalid, the module of the server performing the check may direct that the encrypted message be discarded (Specification, p. 2, lines 11-23). As a result, no encrypted messages are delivered without proof that the associated secret encryption key is escrowed.

In one aspect of the invention, a method for encrypting a message to be transmitted over a network comprises the steps of: encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

In another aspect of the invention, an apparatus for encrypting a message to be transmitted over a network comprises a processor-based device for encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities, wherein the encrypted message is transmitted through the network to a recipient, and in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

In still another aspect of the invention, an article of manufacture comprises one or more software programs for use in encrypting a message to be transmitted over a network, wherein the one or more software programs when executed implement the step of encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities, wherein the encrypted message is transmitted through the network to a recipient, and wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

FIG. 1 shows an illustrative embodiment of an information processing system in which the present invention is implemented. FIG. 2 is a block diagram of one possible implementation of a given one of the elements of the system of FIG. 1. FIGS. 3-6 show flow diagrams of an encyption process, decryption process, proof generation process, and proof verification process, respectively, implemented by elements of the FIG. 1 system in accordance with the invention.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-18 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereinafter "Brickell").

ARGUMENT

Appellant incorporates by reference herein the disclosures of all previous responses filed in the present application, namely, responses dated November 22, 2004 and May 31, 2005.

Rejection under 35 U.S.C. §102(b) over Brickell

Claims 1-3, 5-8, 10, 13, 14 and 16-18

Appellant initially notes that the Manual of Patent Examining Procedure, Eighth Edition, August 2001 (MPEP) §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Independent claim 1 is as follows:

> A method for encrypting a message to be transmitted over a network, wherein the method comprises the steps of:
>
> encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and
>
> transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

In formulating the §102(b) rejection of this claim, the Examiner argues that the elements beginning with the words "encrypting" and "transmitting" are taught by Brickell at col. 6, line 57 though col.

7, line 15 (Final Office Action, p. 3). Appellant respectfully disagrees. The referenced portion of Brickell states:

> In practice it is contemplated that users will also encrypt messages using a symmetric key encryption system. The sender, u, will encrypt a message using a public encryption key (E_u) of the intended recipient, and the recipient will decrypt the message using its corresponding private decryption key (D_u). Analogous to operation of signature/verification keys, messages encrypted using a public encryption key (E_u) can only be decrypted with a corresponding private decryption key (D_u).
>
> As will become readily apparent to one skilled in the art, the foregoing RCA 20 can be used to certify encryption keys in the same manner as is described herein for certifying verification keys. Each user holds its signature key (S_u) and decryption key (D_u) in secret, while allowing distribution and certification of the corresponding verification key (V_u) and encryption key (E_u). It will be appreciated that the security and assurance provided by the user's signature and/or encryption relies in part on the security provided by the signatures of the hierarchy of certifying authorities. Security of signatures relies, in turn, primarily on the cryptographic strength of the signature scheme and on the safety of the private signature keys. It will therefore be appreciated that a compromise of the RCA signature key (also called the "root" key) would destroy the security of the entire system. The root key thus becomes a high-value target for attack by criminals, foreign agents, and hackers.

Appellant submits that one skilled in the art will immediately recognize that this portion of Brickell fails to describe all the elements of claim 1. For instance, Brickell does not describe the use of a "proof of correctness" to indicate "that the message is of a type that allows decryption by one or more escrow authorities." Nor does Brickell describe the checking of the "proof of correctness" as the message traverses a network. In fact, the words "proof," "prove," "correct" and "correctness" are not even present in the Brickell reference. As a result, Brickell fails to describe each and every element of claim 1, and, therefore, fails to anticipate claim 1 under §102(b).

In response to this argument, the Examiner further argues that the "proof of correctness" in the present invention is equivalent to Brickell's method for verifying digital signatures (Final Office Action, p. 2). More specifically, the Examiner states:

> The term "proof of correctness" can be interpreted as 'verifying that a certifying authority is correct by presented (*sic*) to a higher tier certifying authority which issues a certificate,

> authenticating the signature' see [Brickell] col. 3, lines 60-65. The certifying authorities verify that the 'message is a type that allow (*sic*) decryption by one or more escrow authorities' is (*sic*) inherent with the communication described between the plurality of hierarchical certifying tier (*sic*), that certify the digital signature.

Appellant again respectfully disagrees. Brickell at col. 3, lines 58-65, explains such method as follows:

> [A] signature certificate for a user is obtained from a certifying authority at a first tier of the hierarchical digital signature system. The signature certificate from the first tier certifying authority is then presented to a higher tier certifying authority which issues a certificate authenticating the signature of the first tier certifying authority. The user then presents a verifier with the authenticating certificate of the higher tier certifying authority.

One skilled in the art will immediately recognize that Brickell's method comprises the authentication of digital signatures by a certifying authority at the moment of issuance of the digital signature. In claim 1, on the other hand, the "proof of correctness," which guarantees that an encrypted message can be decrypted by an escrow authority, is "checked by at least one module of a server of the network" as the encrypted message traverses the network. Brickell and claim 1 therefore describe entirely different functions to be performed by entirely different entities, i.e., a certifying authority vs. a network server. Brickell, as a result, fails to describe each and every element of claim 1.

Dependent claims 2, 3, 5-8, 10, 13, 14 and 16 are believed allowable for at least the reasons identified above with regard to claim 1. Moreover, the Examiner states that independent claims 17 and 18 are rejected "along the same rationale" as claim 1 (Final Office Action, p. 6). Appellant, therefore, also respectfully submits that independent claims 17 and 18 are in position for allowance for at least the same reasons put forth above with respect to claim 1.

Claim 4

Appellant respectfully submits that dependent claim 4 should be allowed for at least the reasons stated above for claim 1. Moreover, claim 4 contains additional separately patentable subject matter over Brickell.

Claim 4 sets forth "[t]he method of claim 3 wherein the proof of correctness comprises a proof of knowledge of (α, k) that does not reveal y_d^{α} or g^k." In formulating the §102(b) rejection of this claim, the Examiner states that claim 4 is anticipated by Brickell at col. 7, lines 1-5 (Final Office Action, p. 4). This portion of Brickell states:

> Each user holds its signature key (S_u) and decryption key (D_u) in secret, while allowing distribution and certification of the corresponding verification key (V_u) and encryption key (E_u).

Upon reading this portion of Brickell, one skilled in the art will immediately recognize that Brickell merely describes the distribution and certification of private and public keys. In contrast, claim 4 describes a proof of correctness performed by a network server. Because these are entirely different entities, Brickell fails to describe each and every element of claim 4, and the §102(b) rejection of claim 4 should be withdrawn.

Claim 9

Appellant respectfully submits that dependent claim 9 should be allowed for at least the reasons stated above for independent claim 1. Moreover, claim 9 contains additional separately patentable subject matter over Brickell.

Claims 9sets forth the mathematics for determining an embodiment of a proof of correctness in accordance with this invention. In formulating the §102(b) rejection of this claim, the Examiner references a large portion of Brickell, namely col. 21 line 66 through col. 22, line 65. Without reproducing this portion of Brickell here, Appellant asserts that this portion of Brickell describes mathematically a method by which multiple signing unit administrators and signing officers can collaborate to generate an encryption key. Unlike claim 9, it therefore fails entirely to describe the mathematical means in which a proof of correctness is generated, the proof of correctness being checked by a server in a network and being useful to indicate whether an escrow authority can decrypt a message.

For these reasons, Appellant respectfully asserts that claim 9 is not anticipated by Brickell and that the §102(b) rejection should be withdrawn.

Claim 11

Appellant respectfully submits that dependent claim 11 should be allowed for at least the reasons stated above for independent claim 1. Moreover, claim 11 contains additional separately patentable subject matter over Brickell.

Claims 11 sets forth the mathematics for checking an embodiment of a proof of correctness in accordance with this invention. In formulating the §102(b) rejection of this claim, the Examiner references a large portion of Brickell, namely col. 21 line 66 through col. 22, line 65. Without reproducing this portion of Brickell here, Appellant asserts that this portion of Brickell describes mathematically a method by which multiple signing unit administrators and signing officers can collaborate to generate an encryption key. Unlike claim 11, it therefore fails entirely to describe the mathematical means in which a proof of correctness is checked, the proof of correctness being checked by a server in a network and being useful to indicate whether an escrow authority can decrypt a message.

For these reasons, Appellant respectfully asserts that claim 11 is not anticipated by Brickell and that the §102(b) rejection should be withdrawn.

Claim 12

Appellant respectfully submits that dependent claim 12 should be allowed for at least the reasons stated above for independent claim 1. Moreover, claim 12 contains additional separately patentable subject matter over Brickell.

Claim 12 sets forth "[t]he method of claim 1 wherein if the check of the proof of correctness indicates that the proof is invalid, the module of the server directs that the encrypted message be discarded." In formulating the §102(b) rejection of claim 12, the Examiner states that claim 12 is anticipated by Brickell at col. 7, lines 25-34 (Final Office Action, p. 5). This portion of Brickell states:

> An attacker who wants to forge the root signature by obtaining the root key through physical means must penetrate the security of multiple RCA members. If an attacker succeeds in obtaining only a limited number of key shares, the attacker will not be able to reconstruct the root key. Although the system could continue to operate securely, steps would be taken, in accordance with the system and method of the present invention, to respond to the loss or compromise of one or more fragments.

Appellant respectfully submits that this portion of Brickell describes actions to be taken if the security of multiple root certification authorities (RCA's) is breached. As a result, it fails to teach the discarding of an encrypted message when a network server determines that a "proof of correctness" fails to guarantee that the encrypted message can be decrypted by an escrow authority. Brickell, as a result, does not describe each and every element of claim 12, and the§102(b) rejection should be withdrawn.

Claim 15

Appellant also respectfully submits that dependent claim 15 should be allowed for at least the same reasons stated above for claim 1. Moreover, claim 15 contains additional separately patentable subject matter over Brickell.

Claim 15 sets forth "[t]he method of claim 14 wherein the escrow agent associated with the public key is able to decrypt the encrypted message without exposing a corresponding secret key, using a threshold-based method." In formulating the 102(b) rejection of claim 15, the Examiner states that claim 15 is anticipated by Brickell at col. 10, lines 52-67 (Final Office Action, p. 6), which states:

> One property of the multi-step systems that use the RSA algorithm such as described in the '430 application, is that the private signature group key must be in one piece when it is generated. This presents a "single point of failure" for the system, i.e., a point where the signature group key is susceptible to being copied or otherwise compromised. There are cryptographic techniques that can be used as a starting point to solve this problem. An

> example of such techniques can be found in L. Harn, Group-oriented (t,n) threshold digital signature scheme and digital multisignature, IEE proc. Comm. and Digital Tech., Vol 141, No. 5, Sep. 1994. In accordance with these techniques, signature key fragments can be generated by each member of the group and then the public verification key fragments can be combined into a public group verification key in such a way that the private group signature key is never created.

Appellant respectfully submits that this portion of Brickell describes a technique allowing for the initial creation of a public signature group key without the need to create the corresponding private group signature key. This avoids having the private key be susceptible to being compromised. Claim 15, on the other hand, describes a method of decrypting a message using an existing secret key without having the decryption process expose the private key. Brickell and claim 15, therefore, describe entirely different functions and Brickell fails to anticipate claim 15 under §102(b).

For at least the reasons given above, Appellant respectfully requests withdrawal of the §102(b) rejection of claims 1-18.

Respectfully submitted,

Joseph B. Ryan

Date: September 2, 2005

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

What is claimed is:

1. A method for encrypting a message to be transmitted over a network, wherein the method comprises the steps of:

encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and

transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

2. The method of claim 1 wherein the encrypted message is generated by first selecting a random element k from an interval $[0 \ldots q\text{-}1]$, where q denotes the size of a group G, using modulo p, then computing a symmetric key $K = \text{hash}(g^k \bmod p)$ for a symmetric encryption technique (E, D), where g is a generator of the group G, and finally computing the encrypted message in the form of a ciphertext $M' = E_K(M)$, where M denotes the message being encrypted.

3. The method of claim 1 wherein also associated with the encrypted message is an element $a = y_d^\alpha * g^k$ and an element $b = g^\alpha$, where α is chosen uniformly at random from $[0 \ldots q\text{-}1]$ and y_d is a public encryption key.

4. The method of claim 3 wherein the proof of correctness comprises a proof of knowledge of (α, k) that does not reveal y_d^α or g^k.

5. The method of claim 1 wherein also associated with the encrypted message is a certificate C_d on a public encryption key y_d.

6. The method of claim 5 wherein the encrypted message is considered valid by the module of the server if the proof of correctness is valid and the certificate C_d is valid.

7. The method of claim 6 wherein the certificate C_d is considered valid if it is a valid certificate for encryption.

8. The method of claim 1 wherein the proof of correctness comprises a proof c in the form of a triple $(r, s1, s2)$.

9. The method of claim 8 wherein the proof c is generated using the steps of:

selecting two elements β1 and β2 at random from an interval $[0 \ldots q\text{-}1]$;

computing $r = y_d^{\beta 2}\, g^{\beta 2} \pmod{p}$;

computing $e = \text{hash}(r, a)$;

computing $s1 = \beta 1 + e * \alpha \pmod{q}$;

computing $s2 = \beta 2 + e * k \pmod{q}$; and

outputting the triple $(r, s1, s2)$ as the proof c.

10. The method of claim 2 wherein the encrypted message is decrypted by a recipient using the steps of:

computing $B = b^{x_d} \pmod{p}$, where x_d is a secret key corresponding to a public key y_d;

computing $K = \text{hash}(a/B \bmod p)$; and

computing the message M as $M = D_K(M')$.

11. The method of claim 8 wherein the proof of correctness comprising the proof c in the form of the triple $(r, s1, s2)$ is checked by computing $e = \text{hash}(r, a)$ and verifying that $y_d^{s1} * g^{s2} = r * a^e$.

12. The method of claim 1 wherein if the check of the proof of correctness indicates that the proof is invalid, the module of the server directs that the encrypted message be discarded.

13. The method of claim 1 wherein the network comprises a plurality of servers, and wherein each of at least a subset of the servers includes a module for checking the proof of correctness if the corresponding encrypted message passes through the corresponding server in being transmitted from a sender to the recipient through the network.

14. The method of claim 1 wherein the one or more escrow authorities comprises an escrow authority associated with a public key used for encryption of the message, and wherein the escrow authority associated with the public key is able to decrypt the encrypted message to obtain a plaintext message.

15. The method of claim 14 wherein the escrow agent associated with the public key is able to decrypt the encrypted message without exposing a corresponding secret key, using a threshold-based method.

16. The method of claim 1 wherein associated with the encrypted message is a first element that is generated using a public key of the recipient and can be decrypted by a party holding the corresponding secret key, and a second element that proves that the first element can be decrypted by a party holding the corresponding secret key.

17. An apparatus for encrypting a message to be transmitted over a network, wherein the apparatus comprises:

a processor-based device for encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; wherein the encrypted message is transmitted through the network to a recipient, and in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

18. An article of manufacture comprising one or more software programs for use in encrypting a message to be transmitted over a network, wherein the one or more software programs when executed implement the step of:

encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities;

wherein the encrypted message is transmitted through the network to a recipient, and wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None